Cryptography

1. Alice — plaintext — encryption — cipher text — decryption — Bob

Eve

2. Why- military, day-to-day.

3. Caesar cipher. - substitution of letters of alphabet that are shifted by some fixed number of spaces to yield an encoding alphabet.

X Y Z A B C D E F G H
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
A B C D E F G H I J K

Question: Algorithm for decoding this? How many combinations to check?

EXERCISE: How to make caesar cipher more complicated? (permutation of the alphabet, not just shifts)

4. 16th century diplomat Blaise de Vigenère created a very simple cipher that was only cracked Each letter can be encoded as many letters. (interferes with frequency analysis).

	A B C D E F ...
caesar 1	A B C D E F
caesar 2	B C D E F G
caesar 3	C D E F G H
caesar 4	D E F G H I
	E F G H I J
	F K L M N O.
	⋮
caesar 26	Z A B C D E ...

Encode (DEAF BED) using keyword (CAB).

Keyword: CABC ABC
Plaintext: DEAF BED
Ciphertext: EEBH BFF

C indicates which caesar cipher to use for D, F, D

Unbreakable for 300 years. By brute force difficult. Because each letter in a message can be encoded as any of 26 letters. A given message can be encoded in 26^k ways. 7 letter = 8 billion ways.

Weakness: repeated key. If you guess the key correctly, then done. Repetitions in the ciphertext indicate repetitions in the plaintext and space between repetition of the keyword. Babbage's technique was made public only 100 years later.

- How to improve Vigènere cypher? One-time pad. (random key, longer than ciphertext).

0 1 2 3 ... 9 A B C D E F G H I

0 1 2 3 10 etc.

Add two letters together and take reminder ~~mod~~ 36.
This is called addition modulo a natural number n.
We say two integers $a, b \in \mathbb{Z}$ are congruent modulo n if they have the same reminder mod n. So, if A B $A+B \bmod 36 = 21$ and Z P, then $Z+P \bmod 36 = A+P \bmod 36$.

10 11 36 21

A Z
B P

So A is mapped to the same letter P.

ciphertext A Z
key B P
P P.

5. Symmetric key.

6. Secure key.

7. Enigma machine.

8. Public-key cryptography. The encoding or decoding key is public?

9. Exercise. In your day-to-day life which scheme would you use & why. Would you prefer public or private key?

10. RSA - public key. Rivest Shamir Adelman. 1970s. gcd. - greatest common divisor.
Introduced

- Very easy to find large primes (say 100-200 decimal digits)
- What do you need to do to break this scheme?

Exercise: $p=5, q=11$. What are choices for r? Can I choose $r=3$? If yes, what is a public key then. If no, then choose an appropriate r.

Exercise What is your priate key?

Need to solve $rs \equiv 1 \pmod{(p-1)(q-1)}$

equivalently ~~$px+qy=1$~~. $rx+(p-1)(q-1)y=1$ Solve for $x, y \in \mathbb{Z}$.